ГАОУ ВО «Дагестанский государственный университет народного хозяйства»

Утверждена решением
Ученого совета ДГУНХ,
протокол № 13
от 06 июля 2020 г

Кафедра «Информационные технологии и информационная безопасность»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ»

Направление подготовки

10.03.01 Информационная безопасность,

профиль «Безопасность автоматизированных систем»

Уровень высшего образования -бакалавриат

Форма обучения – очная

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 01D74C9001F08320000000072C4B0002
Владелец: Бучаев Ахмед Гамидович
Действителен: с 19.05.2021 до 19.05.2022

Махачкала – 2020

УДК 004.056
ББК 32.973.202

Составитель – Меджидов Заур Уруджалиевич, кандидат экономических наук, доцент кафедры «Информационные технологии и информационная безопасность» ДГУНХ.

Внутренний рецензент – Раджабов Карахан Якубович, кандидат экономических наук, доцент, декан факультета информационных технологий и управления ДГУНХ.

Внешний рецензент – Абдуллаев Ших-Саид Омаржанович, доктор технических наук, главный научный сотрудник Отдела математики и информатики Дагестанского научного центра Российской академии наук.

Представитель работодателя–Зайналов Джабраил Тажутдинович, директор регионального экспертно-аттестационного центра «Экспертиза».

Рабочая программа дисциплины «Комплексное обеспечение защиты информации объекта информатизации» разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации от 1 декабря 2016 г., № 1515, в соответствии с приказом Министерства образования и науки Российской Федерации от 5.04.2017 г. № 301 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры»

Рабочая программа дисциплины «Комплексное обеспечение защиты информации объекта информатизации» размещена на сайте www.dgunh.ru

Меджидов З.У. Рабочая программа дисциплины «Комплексное обеспечение защиты информации объекта информатизации» для направления подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем». – Махачкала: ДГУНХ, 2020 г. - 17 с.

Рекомендована к утверждению Учебно-методическим советом ДГУНХ 03 июля 2020 г.

Рекомендована к утверждению руководителем основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем», к.пед.н., Гасановой З.А.

Одобрена на заседании кафедры «Информационные технологии и информационная безопасность» 30 июня 2020 г., протокол № 12

Содержание

Раздел 1. Перечень планируемых результатов обучения по дисциплине

Цель дисциплины - сформировать компетенции обучающегося в области комплексного подхода к решению задач информационной безопасности объекта информатизации.

Задачи дисциплины:

- Рассмотреть методологию комплексного анализа угроз информационной безопасности;
- Раскрыть общеметодологические принципы построения комплексных систем обеспечения информационной безопасности;
- Показать особенности методов и средств проектирования систем обеспечения информационной безопасности, методов оценки качества систем и моделей, аттестации средств.

1.1 Компетенции выпускников, формируемые в результате освоения дисциплины «Комплексное обеспечение защиты информации объекта информатизации» как часть планируемых результатов освоения образовательной программы высшего образования

Код компетенции	формулировка компетенции
ОПК	**ОБЩЕПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ОПК-7	Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК	**ПРОФЕССИОНАЛЬНЫЕ КОМПЕТЕНЦИИ**
ПК-4	Способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
ПК-7	Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений
ПК-9	Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности

1.2 Планируемые результаты обучения по дисциплине

код и формулировка компетенции	компонентный состав компетенции		
	знать:	уметь:	владеть:

ОПК-7:способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	З1–принципы и методы организационной защиты информации; З2–принципы организации информационных систем в соответствии с требованиями по защите информации.	У1 – определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; У2 – выявлять уязвимости информационно-технологических ресурсов информационных систем.	В1 – навыками анализа информационной инфраструктуры информационной системы и ее безопасности; В2 – методами выявления угроз информационной безопасности информационных систем.
ПК-4:способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	З1–правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; З2–принципы организации информационных систем в соответствии с требованиями по защите информации.	У1 – определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем; У2 – применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; У3 – пользоваться нормативными документами по защите информации.	В1 – методами формирования требований по защите информации; В2 – методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.
ПК-7:Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обос-	З1–принципы формирования комплекса мер по обеспечению информационной безопасности предприятия (организации); З2–принципы организации информационных систем в	У1 – проводить мониторинг угроз безопасности информационных систем; У2–определять комплекс мер (правила, процедуры, практические приемы,	В1 – методами мониторинга и аудита угроз информационной безопасности информационных систем; В2 – методами анализа и формализации информационных процессов объ-

нования соответствующих проектных решений	соответствии с требованиями по защите информации.	руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем.	екта и связей между ними.
ПК-9:Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	З1–принципы организации информационных систем в соответствии с требованиями по защите информации.	У1 – пользоваться нормативными документами по защите информации; У2 – применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.	В1 – методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

1.3. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины

код компетенции	Этапы формирования компетенций			
	Тема 1. Комплексное обеспечение информационной безопасности: сущность, компоненты и задачи. Тема 2. Состав защищаемой информации.	Тема 3. Автоматизированная информационная система как объект защиты. Тема 4. Управление инцидентами и рисками информационной безопасности.	Тема 5. Управление доступом в автоматизированных системах. Тема 6. Системы анализа защищенности.	Тема 7. Межсетевые экраны и виртуальные частные сети. Тема 8. Системы обнаружения и предотвращения вторжений.
ОПК-7	+	+		
ПК-4		+	+	+
ПК-7		+	+	+
ПК-9	+	+		

код компе-	Этапы формирования компетенций

тенции	Тема 9. Защита электронного документооборота. Тема 10. Особенности защиты информации в базах данных.	Тема 11. Концепция создания защищенных автоматизированных информационных систем. Тема 12. Разработка модели комплексной системы защиты информации.	Тема 13. Организация функционирования комплексных систем защиты информации.
ОПК-7	+	+	
ПК-4			+
ПК-7	+	+	+
ПК-9		+	+

Раздел 2. Место дисциплины в структуре образовательной программы

Дисциплина Б1.Б.30 «Комплексное обеспечение защиты информации объекта информатизации» относится к базовой части Блока 1 «Дисциплины» учебного плана направления подготовки «Информационная безопасность», профиля «Безопасность автоматизированных систем».

Для изучения данной дисциплины необходимы знания, умения и навыки по дисциплинам «Сети и системы передачи информации», «Аппаратные средства вычислительной техники», «Информатика», «Информационные технологии», «Теория информации», «Основы информационной безопасности», «Криптографические методы защиты информации», «Техническая защита информации», «Организационное и правовое обеспечение информационной безопасности», «Программно-аппаратные средства защиты информации», «Безопасность вычислительных сетей», «Проектирование защищенных автоматизированных систем».

Знания, умения и навыки, полученные студентами в рамках данной дисциплины, пригодятся им при написании выпускной квалификационной работы, а также при прохождении производственной и преддипломной практик.

Раздел 3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Объем дисциплины в зачетных единицах составляет **4** зачетные единицы.

Количество академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий), составляет **60** часов, в том числе:

на занятия лекционного типа – **30**ч.

на занятия семинарского типа – **30** ч.

Количество академических часов, выделенных на самостоятельную работу обучающихся – **48** ч.

Форма промежуточной аттестации: экзамен, 36 ч.

Раздел 4. Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий.

№ п/п	Тема дисциплины	Всего академических часов	В т.ч. занятия лекционного типа	В т.ч. занятия семинарского типа:					Самостоятельная работа	Форма текущего контроля успеваемости. Форма промежуточной аттестации
				семинары	Практические занятия	Лабораторные занятия (лабораторные работы, лабораторный практикум)	Коллоквиумы	Иные аналогичные занятия		
1.	Комплексное обеспечение информационной безопасности: сущность, компоненты и задачи	6	2	-	2	-	-	-	2	Тестирование Проведение опроса Подготовка презентации Решение кейс-задачи
2.	Состав защищаемой информации	6	2	-	2	-	-	-	2	Тестирование Проведение опроса Подготовка реферата Проведение деловой игры
3.	Автоматизированная информационная система как объект защиты	8	2	-	2	-	-	-	4	Тестирование Проведение опроса Выполнение письменной работы Выполнение проекта
4.	Управление инцидентами и рисками информаци-	8	2	-	2	-	-	-	4	Тестирование Проведение опроса Выполнение письменной работы

	онной безопасности									Выполнение проекта
5.	Управление доступом в автоматизированных системах	8	2	-	2	-	-	-	4	Тестирование Проведение опроса Выполнение письменной работы Выполнение проекта
6.	Системы анализа защищенности	8	2	-	2	-	-	-	4	Тестирование Проведение опроса Подготовка реферата Проведение деловой игры
7.	Межсетевые экраны и виртуальные частные сети	8	2	-	2	-	-	-	4	Тестирование Проведение опроса Подготовка презентации Проведение деловой игры
8.	Системы обнаружения и предотвращения вторжений	8	2	-	2	-	-	-	4	Тестирование Проведение опроса Выполнение письменной работы Выполнение проекта
9.	Защита электронного документооборота	8	2	-	2	-	-	-	4	Тестирование Проведение опроса Подготовка презентации Решение кейс-задачи
10.	Особенности защиты ин-	8	2	-	2	-	-	-	4	Тестирование Проведение опроса

	формации в базах данных									Выполнение письменной работы Выполнение проекта Практическая работа
11.	Концепция создания защищенных автоматизированных информационных систем	8	2	-	2	-	-	-	4	Тестирование Проведение опроса Подготовка реферата Выполнение творческого задания (групповое/индивидуальное)
12.	Разработка модели комплексной системы защиты информации	12	4	-	4	-	-	-	4	Тестирование Проведение опроса Подготовка реферата Проведение деловой игры Поведение круглого стола
13.	Организация функционирования комплексных систем защиты информации	12	4	-	4	-	-	-	4	Тестирование Проведение опроса Подготовка презентации Проведение круглого стола
	Итого	**108**	**30**		**30**				**48**	
	Экзамен (групповая консульта-	**36**								Контроль

	ция в течение семестра, групповая консультация перед промежуточной аттестацией, экзамен)		
	ВСЕГО	**144**	

Раздел 5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

№ п/п	Автор	Название основной и дополнительной учебной литературы, необходимой для освоения дисциплины	Выходные данные по стандарту	Количество экземпляров в библиотеке ДГУНХ/адрес доступа
I. Основная учебная литература				
1.	Аверченков, В.И.	Служба защиты информации: организация и управление	Москва : ФЛИНТА, 2016. – 186 с.	https://biblioclub.ru/index.php?page=book&id=93356
2.	Лапина М.А., Марков Д.М., Гиш Т.А., Песков М.В., Меденец В.В.	Комплексное обеспечение информационной безопасности автоматизированных систем: лабораторный практикум	Ставрополь: СКФУ, 2016. - 242 с.	http://biblioclub.ru/index.php?page=book&id=458012
3.	Пелешенко В. С., Говорова С. В., Лапина М. А.	Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учебное пособие	Ставрополь: СКФУ, 2017. - 86 с.	http://biblioclub.ru/index.php?page=book&id=467139
Дополнительная учебная литература				
а) Дополнительная учебная литература				
1.	А.В. Душкин, О.В. Ланкин, С.В. Потехецкий и др.	Методологические основы построения защищенных автоматизированных систем: учебное пособие	Воронеж: Воронежская государственная лесотехническая академия, 2013. –258с.	http://biblioclub.ru/index.php?page=book&id=255851
2.	Анисин А.А.	Менеджмент в сфере информационной безопасности	М.:Интернет-Университет Информационных Технологий,2009. -176с.	http://biblioclub.ru/index.php?page=book&id=232981
3.	Гуляев В. П.	Анализ демаскирующих признаков объектов информатизации и технических каналов утечки информации: учебно-методический комплекс	Екатеринбург: Издательство Уральского университета, 2014. - 163 с.	http://biblioclub.ru/index.php?page=book&id=275706
Б) Официальные издания: сборники законодательных актов, нормативно-				

правовых документов и кодексов РФ	
1.	Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации" (с изменениями идополнениями)»
2.	ГОСТ 34.320-96.Информационные технологии. Система стандартов по базам данных. Концепции и терминология для концептуальной схемы и информационной базы. 2001 г. www.standartgost.ru
3.	ГОСТ Р ИСО/МЭК 15026-2002. Информационная технология. Уровни целостности систем и программных средств. 2002 г. www.standartgost.ru
4.	ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. www.standartgost.ru
5.	ГОСТ Р ИСО/МЭК 12119-2000. Информационная технология. Пакеты программ. Требования к качеству и тестирование. 2005 г. www.standartgost.ru
6.	ГОСТ Р ИСО/МЭК ТО 16326-2002. Программная инженерия. Руководство по применению ГОСТ Р ИСО/МЭК 12207 при управлении проектом. 2002 г. www.standartgost.ru
7.	ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. 2008 г. www.standartgost.ru
В) Периодические издания	
1.	Информатика и безопасность
2.	Информационная безопасность. Рецензируемый научный журнал «Проблемы информационной безопасности»
Г) Справочно-библиографическая литература	
1.	Краткий энциклопедический словарь по информационной безопасности https://biblioclub.ru/index.php?page=book_red&id=58393&sr=1

Раздел 6. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины

Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к одной или нескольким электронно-библиотечным системам и к электронной информационно-образовательной среде университета (http://e-dgunh.ru). Электронно-библиотечная система и электронная информационно-образовательная среда обеспечивает возможность доступа обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне ее.

Так как в рамках занятия регулярно поднимаются вопросы соответствия используемых для организации защиты информации технологий соответствующим государственным стандартам, а также другим правовым актам современного российского законодательства, то студентам рекомендуется ознакомление с ресурсами правовых систем (онлайн-версии), а также сайты официальных регуляторов в области информационной безопасности:

– http://www.consultant.ru/ Информационно-правовая система "КонсультантПлюс";
– http://www.garant.ru/ Информационно-правовая система "Гарант";
– http://rkn.gov.ru/ Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций;
– http://fsb.ru/ Федеральная служба безопасности;
– http://fstec.ru/ Федеральная служба по техническому и экспортному контролю.

Для самостоятельного изучения материала и ознакомления с новинками в области информационной безопасности рекомендуется использовать следующие Интернет-ресурсы:

1. http://www.ixbt.com
2. http://www.intuit.ru
3. http://www.itsec.ru
4. http://www.iso27000.ru
5. http://www.infosec.ru/
6. http://www.infosecurity.ru/
7. http://www.securrity.ru/
8. http://xakep.ru/
9. http://www.ferra.ru/
10. http://www.3dnews.ru/

Раздел 7. Перечень лицензионного программного обеспечения, информационных справочных систем и профессиональных баз данных

7.1. Необходимый комплект лицензионного программного обеспечения:

1. Windows 10
2. Microsoft Office Professional
3. Adobe Acrobat Reader DC
4. VLC Media player
5. 7-zip
6. ПАК Соболь
7. МДЗ-Эшелон
8. Dallas Lock 8.0-K
9. «ФИКС»
10. «Terrier-2.0»
11. «Ревизор-1 XP»
12. «Ревизор-2 XP»
13. Microsoft Visio Professional 2019
14. Программное обеспечение ViPNet
15. Kaspersky Endpoint Security

7.2.Перечень информационных справочных систем:

– Справочно-правовая система «КонсультантПлюс».

7.3. Перечень профессиональных баз данных:

– Государственный реестр сертифицированных средств защиты информации № РОСС RU.0001.01БИ00 (http://fstec.ru/ tekhnicheskayazashchitainfor-

matsii/dokumenty-po-sertifikatsii/153-sistemasertifikatsii/591-gosudarstvennyj-reestr-sszi).

- Государственный реестр сертифицированных средств защиты информации (http://clsz.fsb.ru/certification.htm);
- Научная электронная библиотека «Elibrary» (https://elibrary.ru);
- Реестр операторов, осуществляющих обработку персональных данных (https://rkn.gov.ru/personal-data/register/).

Раздел 8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для преподавания дисциплины «Комплексное обеспечение защиты информации объекта информатизации» используются следующие специальные помещения– **учебные аудитории**:

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации № 4.9 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»).

Перечень основного оборудования:

Комплект специализированной мебели.

Доска меловая.

Набор демонстрационного оборудования: проектор, персональный компьютер с доступом к сети Интернет и корпоративной сети университета, ЭБС «Университетская библиотека ONLINE» (www.biblioclub.ru), ЭБС «ЭБС Юрайт» (www.urait.ru), интерактивная доска, акустическая система.

Перечень учебно-наглядных пособий:

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики).

Компьютерный класс, учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации № 4.13 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 2 литер «В»).

Перечень основного оборудования:

Комплект специализированной мебели.

Доска меловая.

Набор демонстрационного оборудования: проектор, акустическая система.

Персональные компьютеры – 20 ед.

Программно-аппаратные комплексы ViPNet

Перечень учебно-наглядных пособий:

Комплект наглядных материалов (баннеры, плакаты);

Комплект электронных иллюстративных материалов (презентации, видеоролики).

Помещение для самостоятельной работы № 4.5 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус

№ 2 литер «В»)

Перечень основного оборудования:

Персональные компьютеры с доступом к сети «Интернет» и в электронную информационно-образовательную среду – 19 ед.

Помещение для самостоятельной работы № 1-1 (Россия, Республика Дагестан, 367008, г. Махачкала, ул. Джамалутдина Атаева, дом 5, учебный корпус № 1)

Перечень основного оборудования:

Персональные компьютеры с доступом к сети «Интернет» и в электронную информационно-образовательную среду – 60 ед.

Раздел 9. Образовательные технологии

При освоении дисциплины «Комплексное обеспечение защиты информации объекта информатизации» используются следующие образовательные технологии:

–деловые игры для выработки навыков принятия командных решений;

–лабораторные работы для экспериментальной работы с аналоговыми моделями реальных объектов, а также закрепления теоретического материала при решении практических задач;

–практическое занятие на основе кейс-метода для анализа конкретных ситуаций и задач, поиска верного подхода к их решению;

–внеаудиторная работа в форме обязательных консультаций и индивидуальных занятий со студентами (помощь в понимании тех или иных моделей и концепций, подготовка рефератов, а также тезисов для студенческих конференций и т.д.).

Лист актуализации рабочей программы дисциплины
«Комплексное обеспечение защиты информации объекта информатизации»

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «22» мая 2021 №10
Зав. кафедрой Галяв В.С.

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «____»_____20___ №___
Зав. кафедрой_____

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «____»_____20___ №___
Зав. кафедрой_____

Рабочая программа пересмотрена,
обсуждена и одобрена на заседании кафедры

Протокол от «____»_____20___ №___
Зав. кафедрой_____